APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/516,715	12/02/2004	Joe Howard	P15322-US1	9914

27045　7590　08/30/2006	EXAMINER
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR C11 PLANO, TX　75024	LY, NGHI H

ART UNIT	PAPER NUMBER
2617	

DATE MAILED: 08/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 June 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>11-20</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>11-13 and 15-20</u> is/are rejected.

7)☒ Claim(s) <u>14</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　　1.☐ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

The Art Unit location of your application in the USPTO has changed. To aid in correlating any papers for this application, all further correspondence regarding this application should be directed to Art Unit 2617.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed 06/29/06 have been fully considered but they are not persuasive.

On page 7 of Applicant's remarks, Applicant argues that Matsumoto fails to teach claim 11 and Matsumoto, column 2, lines 11-24, only describes the conventional prior art procedure for the exchange of encryption keys between devices **prior to** the exchange of encrypted messages between such devices. In contrast, Applicant's invention solves a problem in such prior art solutions when it is determined **after** an encrypted message has already been sent/received that the receiving device does not have the necessary key to decrypt the message.

The Examiner, however, disagrees, Matsumoto does indeed teach Applicant's invention in such when it is determined **after** an encrypted message has already been sent/received that the receiving device does not have the necessary key to decrypt the message (see Matsumoto, column 4, line 59 to column 5, line 10, see *"For instance, the user chooses whether a conversation message should be encrypted or not by pressing an on/off command button shown by the GUI (Graphic User Interface). When the encryption mode is on, the encrypting means attaches an encryption flag at the beginning of the encrypted conversation message. The communication device adds a send command to the conversation message, and **sends** them to the network. When*

the receiving user terminal does not have an encryption key to decrypt the encrypted

conversation message, or when the encryption key that the receiving user terminal has

*cannot decrypted the **received** encrypted conversation message"*....That is, the

message has already been sent/received **before** the receiving device does not have

the necessary key to decrypt the message *or* **after** the message has already been

sent/received, the receiving device is determined if it has the necessary key to decrypt

the message). Therefore, the Examiner believes the combination of Reich and

Matsumoto does indeed teach Applicant's claimed invention.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 11, 15, 16, 18 and 20 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Reich et al (US 2002/0184256 A1) in view of Matsumoto et al (US

6,711,264).

Regarding claims 11, 18 and 20, Reich teaches a method of controlling a

network entity of a mobile communication network and a mobile station (see Abstract

and see fig.1, wireless connection between mobile station 12 and network), wherein the

network entity and the mobile station are adapted to conduct a plurality of

predetermined message exchange procedures in the course of which predetermined

messages are exchanged between the network entity and the mobile station depending

on the given procedure (see Abstract, [006], and [0065], see "message"), where the

predetermined messages may be encrypted (see [003], see "encryption"), an encrypted

message being any message of which at least a part is encrypted (see [0064], see

"encrypt"), and where the network entity and the mobile station are adapted to conduct

one or more encryption key generation procedures during which the network entity and

the mobile station generate and store respective corresponding encryption keys in order

to be able to encrypt and decrypt exchanged messages (see [0064], see "encrypt" and

see Abstract, [006], and [0065], see "message"), the method comprises the steps of:

if the network entity receives a message from the mobile station, determining

whether the received message is encrypted (see [0064], see "encrypt" and see

Abstract, [006], and [0065], see "message").

Reich does not specifically disclose if the received message is encrypted,

determining whether a correct encryption key for decrypting the message is available to

the network entity and, if no correct key is available, sending a predetermined triggering

message to the mobile station, and

upon receiving the predetermined triggering message, the mobile station

interrupting the procedure in the course of which it sent the encrypted message for

which the network entity did not have a correct key, and initiating an encryption key

generation procedure.

Matsumoto teaches if the received message is encrypted (see column 2, lines

11-13, see "*generating an encryption key*", in order to generate an encryption key to

decrypt the message, the teaching of Matsumoto inherently teaches "message is

encrypted". In addition, column 2, lines 11-15, see "*adapt to encrypt and decrypt*

communication contents"), determining whether a correct encryption key for decrypting

the message is available to the network entity and, if no correct key is available (see

column 2, lines 11-13, see "*generating an encryption key at at least one of the*

communication devices", in order to generate an encryption key at at least one of the

communication devices, the teaching of Matsumoto inherently teaches "if no correct key

is available", "to the network"), sending a predetermined triggering message to the

mobile station (see column 2, lines 15-22, see "*requesting the encryption key*" or "*upon*

receiving the request". The "request" or "requesting" reads on Applicant's "triggering

message"), and

upon receiving the predetermined triggering message (column 2, lines 15-22, see

"*upon receiving the request*". The "request" or "requesting" reads on Applicant's

"triggering message"), the mobile station interrupting the procedure in the course of

which it sent the encrypted message for which the network entity did not have a correct

key (see column 2, lines 11-13, see "*generating an encryption key at at least one of the*

communication devices", in order to generate an encryption key at the communication

devices, the teaching of Matsumoto inherently teaches "the network entity did not have

a correct key", or if the network already had the key, the communication devices of

Matsumoto does not need to generate a key), and initiating an encryption key

generation procedure (column 2, lines 19-22, see "*generated encryption key*". In

addition, see Matsumoto, column 4, line 59 to column 5, line 10, see "*For instance, the*

user chooses whether a conversation message should be encrypted or not by pressing

an on/off command button shown by the GUI (Graphic User Interface). When the

encryption mode is on, the encrypting means attaches an encryption flag at the

beginning of the encrypted conversation message. The communication device adds a

*send command to the conversation message, and **sends** them to the network. When*

the receiving user terminal does not have an encryption key to decrypt the encrypted

conversation message, or when the encryption key that the receiving user terminal has

*cannot decrypted the **received** encrypted conversation message"*....That is, the

message has already been sent/received **before** the receiving device does not have the

necessary key to decrypt the message *or* **after** the message has already been

sent/received, the receiving device is determined if it has the necessary key to decrypt

the message).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to provide the teaching of Matsumoto into the system of

Reich in order to improve security of communications (see Matsumoto, column 1, lines

7-9).

Regarding claim 15, Reich further teaches the one or more encryption key

generation procedures comprise obtaining an encryption base value commonly

available to the network entity and the mobile station at the time of conducting the

encryption key generation procedure, and generating corresponding encryption keys in

the network entity and the mobile station on the basis of the encryption base value (see

[0064] and [0066]) or (see Matsumoto, column 2, lines 11-25, see *"generated encryption key"*).

Regarding claim 16, Reich further teaches the encryption base value is a regularly changed value that is broadcast by the network to listening mobile stations (see [0064] and [0066]).

4.   Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reich et al (US 2002/0184256 A1) in view of Matsumoto et al (US 6,711,264) and further in view of Pang et al (US 6,931,543).

Regarding claim 12, the combination of Reich and Matsumoto teaches claim 11. The combination of Reich and Matsumoto does not specifically disclose the messages are arranged such that they have a first part and a second part, the first part being an unencrypted part that is not allowed to be encrypted, and the second part being encryptable.

Pang teaches the messages are arranged such that they have a first part and a second part, the first part being an unencrypted part that is not allowed to be encrypted, and the second part being encryptable (see column 4, lines 10-19).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Pang into the system of Reich and Matsumoto in order to prevent data from being loss (see Pang, column 2, lines 33-34).

Regarding claim 13, the combination of Reich and Matsumoto teaches claim 11. The combination of Reich and Matsumoto does not specifically disclose the messages are arranged such that the first part contains an encryption indication of whether the second part is encrypted or not, and the determining of whether the second part of the received message is encrypted or not is achieved by analysing the encryption indication.

Pang teaches the messages are arranged such that the first part contains an encryption indication of whether the second part is encrypted or not, and the determining of whether the second part of the received message is encrypted or not is achieved by analysing the encryption indication (see column 4, lines 10-19).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Pang into the system of Reich and Matsumoto in order to prevent data loss (see Pang, column 2, lines 33-34).

5.   Claims 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reich et al (US 2002/0184256 A1) in view of Matsumoto et al (US 6,711,264) and further in view of D'Amico et al (US 5,077,790).

Regarding claim 17, the combination of Reich and Matsumoto teaches claim 11. The combination of Reich and Matsumoto does not specifically disclose the encryption conducted as a part of a registration procedure of the key generation procedure is mobile station with the network entity.

D'Amico teaches the encryption conducted as a part of a registration procedure of the key generation procedure is mobile station with the network entity (see column 1, lines 65 to column 2, line 6).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of D'Amico into the system of Reich and Matsumoto in order to a method for registration of a portable unit maybe utilized in a communication system the comprises a network controller (see D'Amico, column 1, lines 41-43).

Regarding claim 19, the combination of Reich and Matsumoto teaches claim 18. The combination of Reich and Matsumoto does not specifically disclose the controller is arranged to conduct the encryption key generation procedure as a part of a registration procedure of the mobile station with the mobile communication network.

D'Amico teaches the controller is arranged to conduct the encryption key generation procedure as a part of a registration procedure of the mobile station with the mobile communication network (see column 1, lines 65 to column 2, line 6).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of D'Amico into the system of Reich and Matsumoto in order to a method for registration of a portable unit maybe utilized in a communication system the comprises a network controller (see D'Amico, column 1, lines 41-43).

Allowable Subject Matter

6.   Claim 14 is objected to as being dependent upon a rejected base claim, but

would be allowable if rewritten in independent form including all of the limitations of the

base claim and any intervening claims.

Regarding claim 14, claim 14 is objected for the reasons as stated in previous

Office action, page 7 (dated 10/19/05).

Conclusion

7.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Nghi H. Ly whose telephone number is (571) 272-7911.

The examiner can normally be reached on 8:30 am-5:30 pm Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Nghi H. Ly